13 | 隐私：在实践中如何保护用户隐私？

2020-12-07 郭朝斌

物联网开发实战 进入课程 >

讲述：郭朝斌
时长 20:38 大小 18.90M

你好，我是郭朝斌。

在前三讲中，我带你完善了对物联网系统的**数据技术体系**的认知，包括处理框架、存储方式和设备接入等。

这些内容涉及到很多**大数据技术**，比如基于数据分析结果，提前调度共享单车的位置；还有基于你的搜索记录和购买历史，向你推荐商品。

在**大数据时代**，还有一个话题也是我们非常关心的，那就是这一讲要说的**数据隐私**。这个话题涉及的技术知识点不多，所以你学起来会相对轻松一些。

为什么要了解隐私？

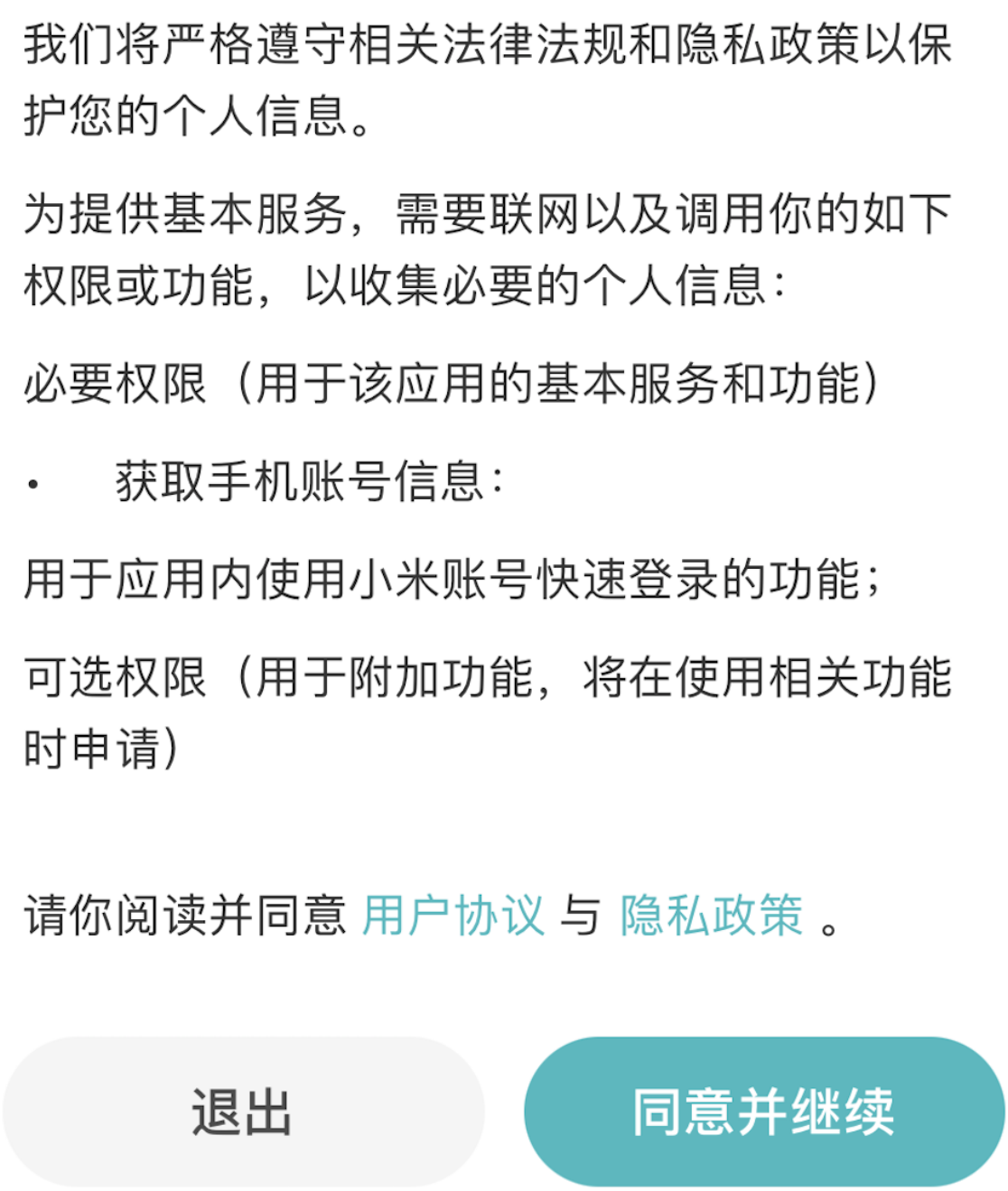
不过，你可能还是要问了：在这个技术类的课程中，为什么要讲这个跟技术关系没那么大的内容呢？作为开发人员，有必要了解这些吗？

其实这样安排有三个原因。

第一，面对产品的需求和设计时，我们最好能做到“知其所以然”。

因为只有这样，才能更好地审视需求，在完成工作的同时，也能提升对业务的理解。

比如，你在手机上新安装了一个应用，打开之后很可能会看到一个隐私条款的弹框。你可以参见下面的图片：



当产品经理向你提出需求，让在你开发的产品中增加这个弹框的时候，你可能会想：为什么要多此一举，设计一个只能同意的隐私条款弹框呢？难道产品同学今天没休息好，怎么关于用户体验的经验还不如你？但是学完这一讲，你就会知道，其实这是隐私法律的要求。

第二，正因为相关的法律法规已经施行，我们需要了解和遵守法律法规，保护用户的隐私数据。

一方面，这要求你在系统开发中采取必要的措施保证数据的安全，比如对数据进行脱敏处理；另一方面，虽然你可能接触到非常多的用户数据，但一定不能随便泄露数据，因为这

是违法的。

类似的情况还有金融圈的 P2P 网贷。当初很多开发人员不懂法，网贷公司跑路之后，他们却糊里糊涂地遭受了牢狱之苦，连之前的工资收入也被没收。

近几年，也已经有很多人因为隐私案件而遭遇类似的经历。比如某公司通过违规收集简历，进行个人数据的违法利用，当公安进行查处时，公司所有员工都被牵扯进来。

另外，如果你的产品要出海，那么国外重要市场的隐私政策也得处理好。因为有些国家的法律法规比较成熟，仅仅是数据防护不力就会导致巨额的罚款。

第三，物联网的应用领域（比如智能家居）可能是一个大生态系统，我们也要满足对接平台的政策要求。

我们开发的产品可能要对接到小米等平台上。这些平台一般都有严格的隐私政策（这些政策可能比法律法规的要求更严格），隐私方面的合规检查是产品上架流程的重要一环。这就要求我们对相关政策要求做到心中有数，在产品开发过程中，能够提前做好隐私数据的规划。

什么是隐私数据？

现在你可能要问了：要求这么多，是不是数据相关的功能和应用都不能做了呢？可是为什么我在电商平台上，还是可以看到很多商品推荐信息呢？

这就涉及到对**隐私数据**的定义了。到底什么是隐私数据，什么不属于？在实际的工作中，如何把握这个度呢？只有搞清楚这个关键问题，你才能更好地把握隐私法规，做好数据应用工作。

我先举个例子，你来判断一下。比如，一些平台会收集你的历史消费信息、生活的城市和使用的手机品牌等数据，构建你的“用户画像”，然后给你贴一些标签。

你要是被贴上了“一线城市”“高收入”和“消费频繁”等标签，它们就会觉得你对价格的敏感度低，对平台的粘性高，最后把同样的商品以更贵的价格卖给你。

请问这触犯了隐私法规吗？当然，这其实就是所谓的**“大数据杀熟”**。2018 年，它甚至被评为年度社会生活十大流行语，引起了人们的广泛关注，你我可能都是受害者。

大数据杀熟和商品推荐系统一样，都利用了**用户画像**。但是商品推荐系统是不违法的，在实践中有很多应用，而“大数据杀熟”却被明确禁止，这是为什么呢？

它们的区别主要在于，“大数据杀熟”针对的是**特定的个人**。当个人被区别定价、达成交易时，这就是对特定个人的**数据滥用**。

个人信息（或者说个人数据，不同国家的叫法不同）可以分为**个人隐私信息**和**个人一般信息**，隐私法律法规主要关注的是个人隐私信息，包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息以及 14 岁以下 (含) 儿童的个人信息等。

另外，通过个人一般信息和其他信息的加工处理形成的信息，一旦泄露、非法提供或滥用，可能危害人身和财产安全，或者导致个人名誉等其他损失的，**也属于个人隐私信息**。比如，有人通过一个明星在微博上发布的图片，推测出明星的住址。

而在万物互联的物联网时代，隐私泄露的风险更大。因为各种设备收集的数据都会上传到云平台，数据的维度和数量都比互联网应用更加丰富，比如你身体的各项生理指标、汽车的行驶记录和家里智能摄像头的影像等等。

同时，现在大数据处理技术、挖掘算法，更是可以基于这些对你来说非常敏感的信息，得出其他的敏感信息。比如你的驾驶习惯好不好，经常开车去什么地方，什么时间出入停车场，汽车保险公司肯定非常想知道。

面对这样的趋势，谁也不希望成为隐私泄露的受害者，变成一只“待宰的羔羊”。所以用户自然也会更加注重数据安全，甚至把这一点作为选择物联网产品的关键决策因素。我们国家也在加强隐私相关法规的完善，规范企业在个人信息利用中的行为。

于是，隐私保护的诉求给物联网的产品和服务提出了更高的要求。那么作为产品的设计者和开发者，你在实践过程中应该怎么保护用户的隐私呢？

目前，你在工作实践中，首先要做到的就是隐私合规，也就是满足各个国家和地区的相关法律法规的要求。因为这是硬性要求，是第一步，只有这样，你的产品才可以顺利地销售或者提供服务，否则就要面临下架和罚款等处罚措施。

国内隐私法律法规

我们先关注一下国内的隐私法规情况。

这一讲开头提到的隐私条款弹框，其实就是《信息安全技术 个人信息安全规范》的要求。它是对《网络安全法》的补充，是国内第一个关于个人信息的实践标准。

有法可依之后，公安网安部门已经针对 App 等网络服务进行了多次个人信息违法问题的整治行动，其中就有像联网汽车 App 这样与物联网有关的案例出现。

另外，我国也在积极推进个人信息保护法的制定。在 2020 年 10 月 13 日，《个人信息保护法》草案已经提交到人大常委会讨论。也许在不久的将来，就会有正式的法律落地。

国家	需要重点关注的法律法规	生效时间
中国	《网络安全法》	2017.06
	《信息安全技术 个人信息安全规范》	2018.05
	《个人信息保护法（草案）》	未生效

出海要注意什么？

看完国内的法律法规，我再来介绍一下国外的情况。

国内企业的出海是越来越明显的趋势，尤其物联网行业里面的智能硬件企业，他们借助我国完整的产业链，具有得天独厚的优势。

在出海过程中，关注国外的隐私法律就成为必须做的事。在实践中，你需要重点关注的是几个主要市场的要求。

欧盟：GDPR

我们先看一下欧盟。欧盟的GDPR（General Data Protection Regulation，通用数据保护条例）知名度非常高，全世界都在关注。它对个人数据进行了全生命周期的保护，被称为**全球最严苛**的隐私政策。

在 2018 年 GDPR 生效之后，欧盟马上就依据**数据跨境传输**等原因，给以 Google 为代表的美国企业开出了 5000 万欧元的罚单。GDPR 不仅适用于当地公司，而是对所有在欧盟提供的产品和服务的公司都提出了限制。它要求个人数据必须落地在欧洲的服务器存储，不能随意传输到其他地区。

美国：《加州消费者隐私法》等法案

接着我们再看看美国的情况。美国比较特殊，它是海洋法系，系统法律条文不多，主要靠援引之前判例，而且每个州的自主权也比较大。所以整体来说，美国隐私相关的法律法规是散落在各个州，或者金融、保险、医疗和电信等领域的各种法案当中。

其中，信息产业发达的加州在 2018 年 6 月生效了《加州消费者隐私法》（California Consumer Privacy Act），这是目前美国最全面、最严苛的隐私法规。

另外，美国也有人在推动全国范围隐私法规的建立。比如苹果的库克就建议制定完整的联邦隐私法，当然，这对于 Google 和 Facebook 这些企业是不利的，因为这些企业的服务更依赖个人信息。

出海需要重点关注的法律法规

总体来说，每个国家和地区都有自己的法律体系和发展节奏，而且法律工作本身是一件非常专业的事情。所以你在出海过程中，最好找**靠谱的、有经验的咨询机构**合作，保障产品在法律上不出问题，避免不必要的经济损失。

我整理了一个表格，列举了在个人信息方面，你需要关注的主要国家和地区的法律法规，供你参考。注意，这里“个人信息”“个人数据”和“隐私”三个名词意思差不多，只是不同地方的表述习惯不一样。

国家/地区	需要重点关注的法律法规	生效时间
欧盟	GDPR（《通用数据保护条例》）	2018.05
美国	Privacy Act（《隐私权法》）	1974.12
	Telephone Consumer Protection Act（《电话消费者保护法》）	1991
	HealthInsurance Portability and Accountability Act（《健康保险便利和责任法案》）	1996
	Children"s Online Privacy Protection Act（《儿童网上隐私保护法》）	1998
	Gramm–Leach–Bliley Act（《金融服务现代化法》）	1999
	CAN–SPAM Act（《反垃圾邮件法》）	2003
	Clarifying Lawful Overseas Use of Data Act（《澄清域外合法使用数据法》）	2018.03
	California Consumer Privacy Act（《加州消费者隐私法》）	2018.06
日本	《个人信息保护法》	2005.04
俄罗斯	《信息、信息技术及信息保护法》	2006
	《个人数据保护法》修正案	2014.07
澳大利亚	《隐私法》	1988
	《重要数据泄露应对方案》	2018.02
印度	《个人数据保护法（草案）》	2018.07
巴西	《个人和企业数据保护法案》	2018.08
中国台湾	《个人资料保护法》	2010.04
中国香港	《个人资料（隐私）条例》	2013.04

怎么把握繁多的法律法规？

法律法规的内容非常多，作为行业从业人员，我们也不可能把所有条文都背得滚瓜烂熟。那么，有什么简单的办法来指导日常工作吗？我想，你在实践中可以把握下面这 4 个基本原则。

第一，保证用户有知情权和选择权。

如果需要收集用户的个人信息，我们需要告知用户，征求用户的授权，而且要用显著的、容易懂的方式说明信息的使用方式、使用范围和目的。

比如我刚才提到的隐私信息弹窗就是一个例子。而且，用户还要能够决定是否同意授权，以及授权之后再取消授权。你在做智能硬件配套的 App 时，可以留意这方面的要求。

第二，收集、使用信息时要采用最小必要原则。

这个比较好理解。我们收集使用的信息应该尽量少，只要能够满足产品和服务的功能需求就足够了。比如智能台灯，我们只需要接收的房间信息就可以实现语音控制和交互，并不需要收集准确的 GPS 定位。

第三，保证用户有信息控制自主权。

我们收集的信息的主体仍然是用户，也就是说，用户随时可以查看自己的数据，可以修改、甚至删除它们。你可以在 App 或者网页中提供这样的入口。

第四，确保个人信息存储和使用的安全。

收集了用户的个人信息，我们就需要保证个人信息的数据安全，从内部人员的管理和数据的使用流程上把控风险，比如将数据中的个人指向性内容去掉。同时，我们也要做好系统的安全防护工作，防止被攻击导致数据泄露。在下一讲中，我还会讨论更多关于系统安全的内容。

从这些原则出发，你就可以更好地理解和满足相关法律法规的要求，做好产品和服务的合规工作。

从用户的角度出发的设计

以上内容主要是从法律角度来讨论这个问题。但是从根本上说，你还是需要从用户的角度出发，在为用户创造价值和解决问题的同时，保护好用户的隐私。

法律永远是滞后的，法律也总有漏洞，各种利用个人隐私信息获利的新方法会不断出现。但是用户会“用脚投票”，选择隐私保护更好，更值得信赖的产品和服务。从这个角度考虑，隐私保护虽然需要企业投入成本，但是它也可以成为企业独特的竞争优势。

比如，国外有一个搜索引擎公司 DuckDuckGo，在棱镜门事件后，日均使用量一年就翻了一倍，近几年用户量也是稳步增长，2020 年 8 月用户量就达到了 6500 万。它吸引用户的一个关键点正是强调用户隐私，不追踪用户，也就是**匿名性**。这和 Google 这样的搜索引擎恰恰相反。

除了匿名，你还可以像苹果公司一样采用“**差别隐私**”的方法，通过在数据中增加“噪音”，或者修改数据隐私信息，来保护用户的个人信息泄露。

我再举一个互联网应用的例子，因为你日常中接触得更多。

当你在微信中分享照片，无论通过聊天界面还是朋友圈，微信一般都会对照片进行压缩。有时候你可能还会抱怨微信把照片处理得不够清晰，所以专门选择发送原图。

其实微信在压缩照片的同时，都会修改照片的 **EXIF 信息**，它包含拍摄时间、地点等隐私信息。如果你的照片被“有心人”利用，他们可能通过数据分析，直接精确地定位到你家小区，是不是很可怕？

其实微信还有很多类似的从用户角度出发的设计。比如微信朋友圈中的“给谁看”“不给谁看”“仅自己可见”等，就是**给用户控制数据可见范围的选项**。这样用户会更有控制感。

另外，可以**减少信息的展示时间，甚至避免信息的永久存储**。最知名的就是聊天软件上的“阅后即焚”功能。还有微信中聊天记录不会被云端永久保存，朋友圈中的“三天可见”“半年可见”，也是同样的设计思路。这种设计可以让用户更放心地分享内容，提高用户体验的同时，也增强了产品的粘性。

那基于同样的思路，在硬件上我们也可以多采取类似的产品设计方法和角度，提高用户的信任感。

比如，智能手表设备会收集很多用户的个人生理指标数据，而且一般在设备上有数据的存储功能。这种存储当然出发点是为了缓存数据，保证数据在手机或者云端的可靠获取，但是它也存在泄漏的风险。

那我们就可以增加一个功能，让用户可以随时通过手表本身，不用借助手机等其他设备就可以永久删除存储的历史数据。这样的设计会让用户更加放心地使用产品。

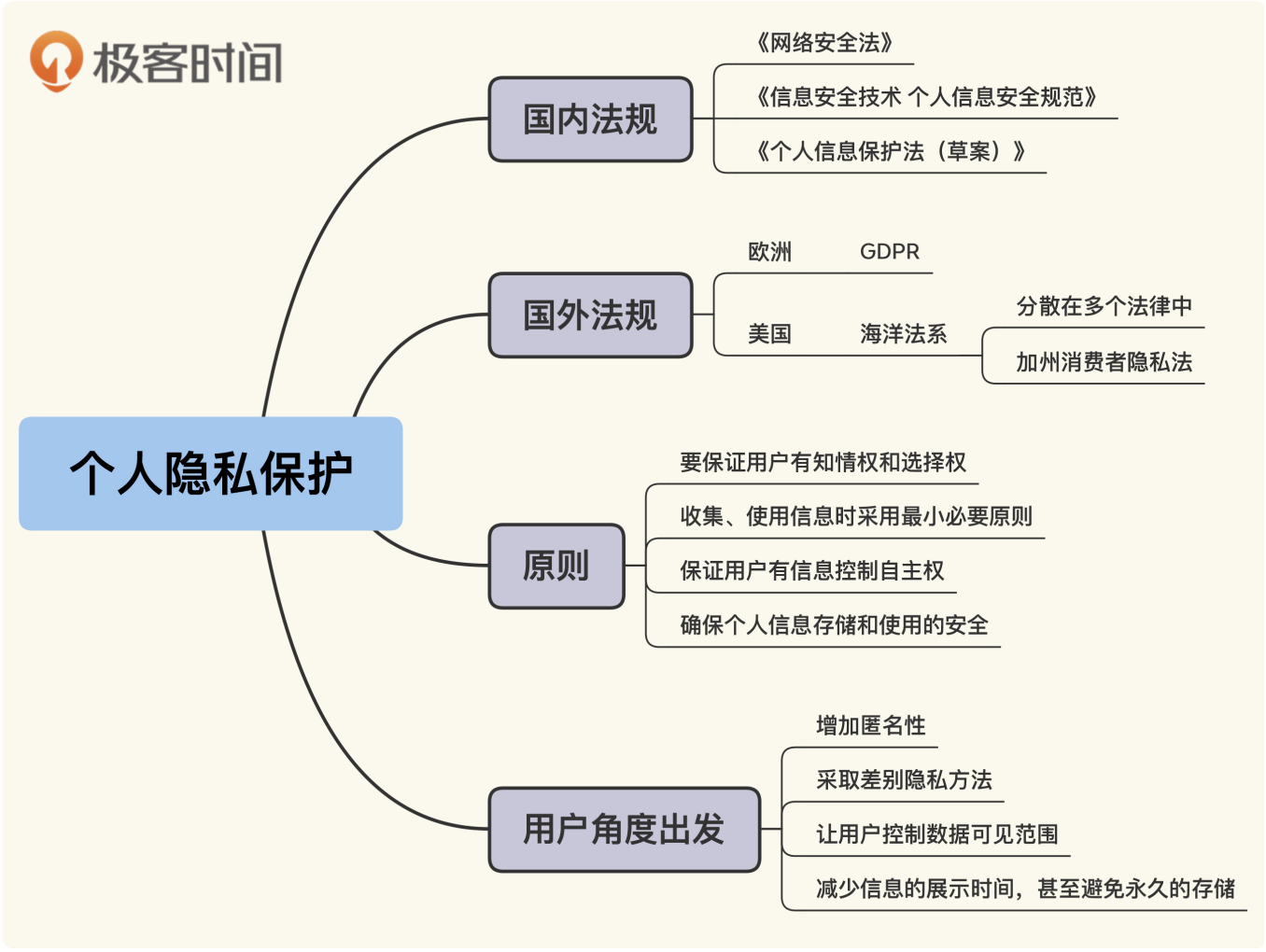
小结

总结一下，在这一讲中，我分析了学习隐私知识的必要性，重点讲解了隐私数据的概念，并介绍了国内、国外关于用户隐私的法律法规和把握这些法规的基本原则。

除了法律法规，我也谈了从用户角度出发，做好隐私保护工作的思路和方法。了解了这些，你才能在物联网行业从业过程中做好合规工作，并且设计出让用户真正感到满意和放心的功能。

1. 从懂业务、懂法律和懂生态的角度，我们作为开发人员都需要掌握隐私的相关知识。
2. 在隐私法规上，个人信息可以分为个人隐私信息和个人一般信息。我们需要重点关注个人隐私信息的保护。
3. 在隐私保护方面，我国已经生效的法律有《网络安全法》和《个人信息安全规范》。另外，《个人信息保护法》的草案已经提交人大常委会讨论，在不久的将来应该也会正式发布。企业出海时，需要关注当地的法律，比如欧盟的 GDPR，以及美国各个州和各个领域的相关法案。为了保证出海工作的顺利进行，我们最好还是找专业的咨询机构合作。
4. 作为物联网行业的从业者，在实践中要把握 4 条基本原则：第一，保证用户有知情权和选择权；第二，收集、使用信息时要采用最小必要原则；第三，保证用户有信息控制自主权；第四，确保个人信息存储和使用的安全。
5. 让产品和服务符合法律法规的要求只是第一步。在产品理念，或者说底层价值观上，我们要从用户角度出发，重视对用户隐私的保护。具体的方法有增加匿名性，采取差别隐私，让用户可以控制数据可见范围和减少信息的展示时间甚至避免永久的存储。

我整理了一张思维导图，供你参考。



隐私政策在近几年备受关注，这背后的本质原因，也许是科技的发展、数字化深入生活的必然趋势。用户只有让渡一些个人信息才能获得更好的服务，或者更有利于需求的解决；但是任何时候，用户的个人信息都不应该被滥用、被泄露、被非法提供进行交易。

正如张小龙说的那样：“**善良比聪明更重要，AI 比我们更聪明、更懂套路，但我们可以比他更善良。**”只有这样用户才会信任你，你也才能拥有一个长久的、有生命力的产品和服务。

而如果作为消费者，我们也需要了解这些法律法规的基本信息，保护好个人的隐私数据，并且遇到问题时，把它们作为维护自己权益的工具。

思考题

最后，我给你留一个思考题吧。

智能家居中，用于安全监控的摄像头有很多的价值，但是很多人担心它的安全性，害怕隐私数据的泄露。如果你来设计摄像头产品，从用户的角度出发，会做哪些设计来增加产品

的认可度呢？

欢迎你在留言区写一写自己的思考，也欢迎你将这一讲分享给对隐私保护感兴趣的朋友一起学习。

提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 12 | IoT Hub：面对海量设备如何打造高性能设备接入层？

下一篇 14 | 安全：物联网平台如何应对安全风险？

精选留言 (8)

写留言

qinsi
2020-12-07

对于处于事实垄断地位的app来说，用户的选择权也就是做个形式。另外开篇中提出的用户跟踪问题要怎么解决呢？

展开

作者回复: 所以要靠法律法规来规范企业行为，也要我们普通用户提高隐私保护意识

4

Nior
2020-12-07

配备摄像头开启指示灯、增加物理摄像头挡板、关闭摄像头自动调整摄像头面向墙壁

作者回复: 赞

1 3

YueShi
2020-12-07

智能家居有一个点,
如果我们开着抓包或者其他路由软件,
就会发现有很多莫名其妙的短链接和长链接,
持续不断的发送着信息.
...
展开

作者回复: 这些不一定是个人信息。有些还涉及企业技术的实现细节，不太好这样实施

3 2

il李li
2020-12-07

摄像头连接平台进行身份认证，用户连接平台进行身份认证，用户查看设备先进行双向身份认证，认证技术基于PKI体系，各参与方都有自己的身份证书
展开

作者回复: 嗯，这是企业需要做到的。可以再思考一下，怎么让用户更好感知到这些努力呢?

1 2

Matthew
2020-12-11

增加物理挡板最可靠，简单粗暴管用。用户只信眼睛看到的!

作者回复: 有道理

1

涂满蜂蜜的馒头
2020-12-07

摄像数据本地加密，摄像数据传输加密，摄像数据加密云存储

作者回复: 嗯，这处理成本不低。另外，也可以从用户感知上考虑一下。

1 1

莹

2020-12-20

前期做好用户研究，了解用户关心在哪些方面的隐私，比如房间区域，捕捉内容，是不是希望一直录像，还是只在房间中发生动静时候捕捉，然后将合理的选项提供给用户做决定。

Geek_2c8816

2020-12-07

增加物理开关，让用户选择要不要自动上传云端，不上传的话摄像头存储满了就自动覆盖

作者回复: 赞👍，给用户控制权